CÓDIGOS CONVOLUCIONALES DE PRODUCTO: Propiedades de Distancia, Codificación y Decodificación

Carlos A. Medina C., Ph. D.
Universidad Tecnológica de Panamá
carlos.medina@utp.ac.pa

Vladimir Sidorenko, Ph. D.
Universidad de Ulm
vladimir.sidorenko@uni-ulm

RESUMEN
Existen multiplicidad de métodos bien conocidos para combinar códigos de bloque para corrección de errores. Sin embargo, no son tan diversos los métodos aplicados para la combinación de códigos convolucionales. Por esto, se propone la aplicación del método de producto directo, método tradicional para códigos de bloque, a la construcción de nuevos códigos convolucionales. En este estudio se define e investiga el producto directo aplicado a códigos convolucionales, considerando algunas de las propiedades de las matrices de generación y paridad resultantes, así como la definición de un nuevo concepto de distancia, la "distancia de bloque" para los códigos convolucionales componentes y el código de producto resultante. Además, se consideran algunos métodos para la codificación y decodificación de estos códigos de producto.

Palabras claves: *códigos convolucionales, códigos de producto, distancia de bloque, decodificación iterativa.*

ABSTRACT
There are many well-known methods for combining block codes for error correction. However, they are not as different methods used for combining convolutional codes. Therefore, it is proposed the method of direct product, a traditional method for block codes, to the construction of new convolutional codes. This study defines and investigates the direct product applied to convolutional codes, considering some of the properties of the resulting generation and parity check matrices, and the definition of a new concept of distance, the block distance for components convolutional codes and the resulting product code. Moreover, some methods are considered for coding and decoding of these product codes.

Key words: *convolutional codes, block distance, iterative decoding.*

1. INTRODUCCIÓN

La combinación de códigos conocidos es un método poderoso para obtener nuevos códigos que presenten características ventajosas tales como: grandes distancias, capacidad para corrección de errores en ráfaga y aleatorios, longitudes de bloque grandes, matrices de verificación de paridad de baja densidad, y además, que permitan la decodificación utilizando técnicas con baja complejidad incluyendo métodos iterativos.

Existen muchos métodos bien conocidos para combinar códigos de bloque (ver e.g. [1]). Uno de los primeros métodos para combinación, "*el producto directo*", fue propuesto por Elias [2] en 1954. Dados dos códigos de bloque lineales C para codificación *horizontal* y $C^{|}$ para codificación *vertical*, con longitudes n y $n^{|}$, y distancias de Hamming d y $d^{|}$, respectivamente, el código de producto directo C consiste en todas las matrices $n^{|} \times n$, tales que cada fila pertenece al código horizontal C y cada columna pertenece al código vertical $C^{|}$. La distancia del código C es $d\,d^{|}$.

Para códigos convolucionales son muy pocos los métodos sugeridos para combinarlos. Tal vez uno de los más poderosos métodos, los códigos convolucionales "entretejidos" ("*woven convolutional codes*") ha sido considerado en [3] y [4]. Métodos para combinar códigos convolucionales, similar al producto directo de códigos de bloque, se han sugerido y descrito en [5] y [6].

En este trabajo se brinda una definición algebraica del producto directo de códigos convolucionales y se investigan las propiedades de la codificación, la distancia de dichos códigos, y algunas técnicas para decodificación. La relación entre los códigos convolucionales de producto y los códigos convolucionales entretejidos se discute en [7].

La publicación clásica de Fomey [8] muestra que los códigos convolucionales pueden tratarse como "códigos de bloque" sobre el campo $F'(D)$ de funciones racionales en el indeterminado D sobre cualquier campo finito F. Esto, nos permite definir el producto directo de códigos convolucionales y encontrar sus matrices generadora y de verificación de paridad, en forma similar a los códigos de bloque, de una manera sencilla. En contraste con los códigos de bloque, la distancia libre (*free distance*) de los códigos convolucionales de producto alcanza el producto de las distancias de los códigos componentes (i.e., $d^- d^|$.) solamente si algunas restricciones adicionales se satisfacen. Siguiendo las relaciones con los códigos de bloque, sugerimos el concepto de *distancia de bloque* para un código convolucional. Además, esta distancia resulta importante porque permite la estimación de la distancia libre d_f del código convolucional de producto en forma sencilla. Se estudia la forma de calcular la distancia libre d_f de un código de producto utilizando las distancias de bloque y se muestra que este método resulta en una estimación precisa y simple.

Un código convolucional de producto puede considerarse como una concatenación serial de los códigos componentes y de esta forma, el mismo puede decodificarse utilizando métodos iterativos. Entre ellos, consideramos la decodificación iterativa de códigos concatenados en serie y la decodificación iterativa de producto. En [5] y [6], este último método se denomina filtrado MAP o procesamiento iterativo.

Las siguientes secciones incluyen algunas definiciones importantes para comprender el desarrollo del código propuesto, la forma como codificar el código, las propiedades de las matrices de generación y paridad, la estimación de la distancia libre del código y algunos aspectos sobre la decodificación del mismo.

2. DEFINICIONES

Sea F un campo de Galois (GF), F= GF(q) Así, $F(D)$ denota el campo de funciones racionales sobre F en el indeterminado D (llamado operador de retardo). Cada elemento $a(D)$ distinto de cero de $F(D)$ puede representarse en forma única por un elemento de F como una razón de polinomios en F (i.e., $a(D) = p(D)/q(D)$, donde $p(D)$ y $q(D) \neq 0$ y relativamente primos), y cada elemento $a(D)$ puede asociarse en forma única con una serie formal de Laurent de la forma [9]

$$a(D) = \sum_{i \geq m} a_i D^i \qquad (1)$$

donde m puede ser cualquier entero, los coeficientes a_i pertenecen al campo F, y D es una variable formal (indeterminado).
En este estudio nos limitaremos a códigos binarios, i.e., GF(2) denotado F_2.

Definición 1: Un código (n,k) convolucional binario C es un sub-espacio k-dimensional de $\{F(D)\}^n$, donde F = GF(2), i.e., un sub-espacio del espacio vectorial de n-tuplos en $F_2(D)$. La razón R del código convolucional C se define como $R = k/n$.

Definición 2: Una matriz k x n $G(D)$ cuyas filas forman una base de un código (n,k) convolucional se denomina una matriz generadora del código.

Definición 3: Para cualquier código (n,k) convolucional C, sea $H(D)$ una matriz r x n en $F(D)$ con rango $r = n - k$ tal que $v(D)$ es una palabra código de C si y sólo si

$$v(D)H^T(D) = 0$$

donde T denota el operador transposición. Cualquiera de tales matrices $H(D)$ se denomina una matriz de verificación de paridad del código.

Definición 4: Sean C^- y C$^|$ códigos (n^-,k^-) y ($n^|$,$k^|$) convolucionales, respectivamente; entonces, el producto directo $C^- \otimes$ C$^|$ se define como el código cuyas palabras código consisten de todos los arreglos $n^- \times n^|$, en los cuales las filas pertenecen al código C^- y las columnas al código C$^|$.

Lema 1: El código de producto directo definido es un sub-espacio $k^- k^|$ -dimensional de $F(D)^{n^- n^|}$.

3. CODIFICACIÓN

En esta sección se consideran la forma de codificar el código convolucional de producto y se estudian las características de las matrices generadora y de paridad del mismo.

3.1 Matriz generadora

La codificación del producto directo $C^- \otimes C^|$ de códigos convolucionales puede realizarse de forma similar a la de los códigos de bloque como se indica:

Sean $G^-(D)$ y $G^|(D)$ matrices generadoras del código (n^-, k^-) horizontal C^- y $(n^|, k^|)$ vertical $C^|$, respectivamente. Denote por $U(D)$ una matriz $k^| \times k^-$ de información sobre $F(D)$. Ahora se puede aplicar una codificación "*fila-columna*" (FC); i.e., primero se codifica cada fila de $U(D)$ usando la matriz generadora $G^-(D)$, y se obtiene una matriz $V(D) = U(D)\, G^-(D)$. Luego, cada columna de $V(D)$ se codifica utilizando la matriz generadora $G^|(D)$. Después de esta codificación FC se obtiene

$$C(D) = G^{|T}(D)\left[U(D)G^-(D)\right]. \tag{3}$$

También se puede aplicar una codificación "*columna-fila*" (CF) y obtener la misma multiplicación de matrices en otro orden:

$$C(D) = \left[G^{|T}(D)U(D)\right] G^-(D). \tag{4}$$

En cualquier caso, note que la matriz de la palabra código codificada de producto $C(D)$ está dada por

$$C(D) = G^{|T}(D)U(D)G^-(D). \tag{5}$$

De la ecuación (3) se sigue que cada columna de $C(D)$ pertenece a $C^|$, y de la ecuación (4) que cada fila de $C(D)$ pertenece a C^-, de forma que por la *Definición* 4 se obtiene una *palabra código* $C(D) \in C^- \otimes C^|$. La Figura 1 muestra el proceso de codificación.

Ahora, considere C el conjunto de matrices $C(D)$ obtenido por la codificación de todas las matrices

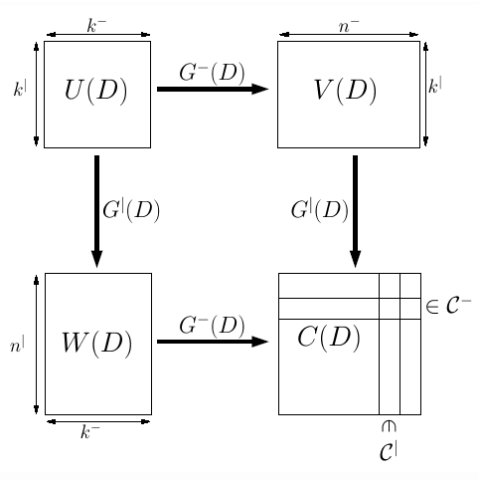

Figura 1. Codificación de un código convolucional de producto.

$U(D)$ usando la ecuación (5). A continuación se demuestra que C es un código $(n^- n^|, k^- k^|)$ convolucional, y que $C = C^- \otimes C^|$. Debemos mostrar que C satisface la *Definición* 1,y que todas las matrices $C(D)$ que satisfacen la *Definición* 4 están incluidas en C.

Para mostrar esto, reemplacemos las matrices $C(D)$ por vectores $\boldsymbol{c}(D)$ como sigue. Sea $row(A)$ un vector obtenido al escribir los elementos de la matriz A fila por fila. Así, reemplazando cada matriz $C(D)$ por el vector $\boldsymbol{c}(D) = row[C(D)]$ obtenemos un código C de vectores. Usando la notación $\boldsymbol{u}(D) = row[U(D)]$ podemos reescribir el procedimiento de codificación dado por la expresión (3) para el código de producto en la forma vectorial tradicional:

$$\boldsymbol{c}(D) = \boldsymbol{u}(D)G(D) \tag{6}$$

donde la matriz generadora $G(D)$ está dada por

$$G(D) = G^|(D) \otimes G^-(D). \tag{7}$$

La derivación de (7) está basada en la siguiente propiedad del producto de Kronecker [10]:

$$row(ABC) = row(B)\left(A^T \otimes C\right) \tag{8}$$

donde A, B y C son matrices con las dimensiones adecuadas y $\otimes$ indica el producto de Kronecker.

Ya que las matrices generadoras $G^{-}(D)$ y $G^{|}(D)$ tienen elementos de $F(D)$, i.e., son matrices racionales, de la expresión (7) se tiene que $G(D)$ también es una matriz racional $k^{-}k^{|} \times n^{-}n^{|}$ de rango completo [10]. Así, el código C generado por $G(D)$ es un sub-espacio $k^{-}k^{|}$ -dimensional de $F(D)^{n^{-}n^{|}}$. Esto significa que todas las matrices $C(D)$ que satisface en la Definición 3 están incluidas en C debido al *Lema* 1. Finalmente, se concluye que el código C generado por la expresiones (5) es

- el producto directo de los códigos convolucionales C^{-} y $C^{|}$;
- un código convolucional ($n^{-}n^{|}$, $k^{-}k^{|}$).

Este código C se denomina un *código convolucional de producto*.

3.2 Matriz de verificación de paridad

Asuma que $H^{-}(D)$ y $H^{|}(D)$ son matrices de verificación de paridad de los códigos componentes. De la *Definición* 3 del código de producto C se tiene que una matriz $C(D)$ $n^{|} \times n^{-}$, pertenece a C si y sólo si las siguientes ecuaciones de verificación de paridad se satisfacen para las filas y columnas de la matriz $C(D)$:

$$\begin{aligned} C(D)H^{-}(D)^{T} &= 0, \\ H^{|}(D)C(D) &= 0. \end{aligned} \tag{9}$$

La ecuación de verificación de paridad (9) puede también rescribirse en forma vectorial usando la ecuación (8) como

$$\boldsymbol{c}(D)H(D)^{T} = 0, \tag{10}$$

donde la matriz de verificación de paridad es

$$H(D) = \begin{pmatrix} I_{n^{|}} \otimes H^{-}(D) \\ H^{|}(D) \otimes I_{n^{-}} \end{pmatrix}, \tag{11}$$

donde I_m corresponde a la matriz identidad $m \times m$. *Observación*: la matriz $H(D)$ tiene filas redundantes y la misma puede reducirse. Si $n^{|}$ o n^{-} es grande, la matriz $H(D)$ es dispersa y se podrían aplicar entonces métodos de decodificación iterativa para códigos LDPC (*low density parity check codes*) a la decodificación de estos códigos de producto.

3.3 Algunas propiedades de la matriz generadora

Utilizando las definiciones de [11] se pueden establecer las siguientes propiedades de la matriz generadora de los códigos convolucionales de producto.

Teorema 2: Sean $G^{-}(D)$ y $G^{|}(D)$ matrices generadoras polinomiales con memoria m^{-} y $m^{|}$, y longitudes de restricción totales v y $v^{|}$, respectivamente. La memoria m y la longitud de restricción total v de la matriz generadora $G(D)$ del código convolucional de producto son

$$m = m^{-} + m^{|} \quad \text{y} \quad v = k^{|}v^{-} + k^{-}v^{|}.$$

Teorema 3: Si $G^{-}(D)$ y $G^{|}(D)$ son matrices generadoras racionales sin retardo, entonces la matriz $G(D)$ del código convolucional de producto es una matriz sin retardo *Teorema* 4: Si $G^{-}(D)$ y $G^{|}(D)$ son matrices generadoras sistemáticas, entonces la matriz $G(D)$ del código convolucional de producto es sistemática.

Teorema 5: Si $G^{-}(D)$ y $G^{|}(D)$ son matrices de codificación básicas mínimas, entonces la matriz $G(D)$ del código convolucional de producto es una matriz de codificación básica mínima.

La matriz generadora del código de producto hereda las propiedades de los códigos componentes. Por lo tanto, si se construye un código convolucional de producto con dos códigos componentes con matrices de codificación básicas mínimas, la matriz generadora resultante será una matriz de codificación no-catastrófica, la forma canónica de controlador de la matriz codificadora será un codificador mínimo y el trellis de Forney correspondiente del código será un trellis mínimo, ya que éstas son propiedades de las matrices de codificación básicas mínimas.

4. ESTIMACIÓN DE DISTANCIA

En esta sección se introduce el concepto de distancia de bloque y la forma como se puede

estimar la distancia libre del código convolucional de producto utilizando este concepto.

4.1 Distancia de bloque

En contraste con los códigos de bloque, la distancia libre d_f de un código convolucional de producto puede resultar menor que el producto $d_f^- d_f^|$ de las distancias libres de los códigos componentes. Para estimar d_f y derivar restricciones para garantizar la "*distancia de producto*"

$$d_f \geq d_f^- d_f^| \tag{12}$$

introducimos el concepto de distancia de bloque de un código convolucional.

Un código C convolucional (n,k) es un conjunto de n-vectores $\boldsymbol{c}$ sobre un campo de series de Laurent $F(D)$, i.e., C puede considerarse como un código de bloque (n,k) sobre el campo $F(D)$. La distancia de Hamming $D_{F(D)}(\boldsymbol{c}_1,\boldsymbol{c}_2)$ entre dos vectores $\boldsymbol{c}_1$, $\boldsymbol{c}_2$ sobre $F(D)$, similar a los códigos de bloque, es igual a el número de posiciones en las que estos vectores difieren.

Definición 4: La distancia de bloque d_B de un código C convolucional (n,k) se define como

$$d_B(C) = \min_{\substack{\boldsymbol{c}_1,\boldsymbol{c}_2 \in C \\ \boldsymbol{c}_1 \neq \boldsymbol{c}_2}} D_{F(D)}(\boldsymbol{c}_1,\boldsymbol{c}_2) \tag{13}$$

Así, d_B es la distancia del código mínima del correspondiente código de bloque lineal C sobre el campo $F(D)$. Ya que el código es lineal, d_B también es igual al peso de Hamming mínimo para todas las palabras distintas de cero.

Para un código C convolucional (n,k) con distancia libre d_f (sobre el campo base F) tenemos

$$d_B \leq n, \tag{14}$$

$$d_B \leq d_f. \tag{15}$$

4.2 Estimación de la distancia libre

Volviendo al código convolucional de producto $C = C^- \otimes C^|$, de la teoría de los códigos de bloque y utilizando la ecuación (15) se obtiene para la distancia libre de C que

$$d_f \geq d_B = d_B^- \times d_B^| \tag{16}$$

donde $d_B^- = d_B(C^-)$, $d_B^| = d_B(C^|)$. El siguiente teorema mejora esta estimación de la distancia libre.

Teorema 6: La distancia libre de C satisface

$$d_f \geq \max\left\{d_B^- d_f^|, d_B^| d_f^-\right\}. \tag{17}$$

Así, si la distancia de bloque de al menos uno de los códigos componentes, por ejemplo el vertical, es igual a su distancia libre, se garantiza la distancia de producto (12).

Sin embargo, la distancia de bloque de un código corto no puede alcanzar su distancia libre debido a (14). Una forma de superar este problema es utilizar un código convolucional *bloqueado*. Otra forma, no discutida aquí, es utilizar códigos componentes con, por ejemplo, $n^| \geq d_f^|$ y $d_B^| = d_f^|$.

El procedimiento de bloqueo [3], [12] no cambia un código convolucional (n,k) como el conjunto de símbolos sobre el campo base F. Bloquear un código con un factor de bloqueo M sólo junta bloques de símbolos de longitud n en bloques de longitud Mn, resultando un código (Mn, Mk) que es esencialmente el mismo código denotado por $C_{[M]}$.

La distancia de bloque de un código convolucional típicamente crece con el factor de bloqueo M hasta que la distancia alcance d_f ; de forma que se puede establecer el siguiente teorema.

Teorema 7: El límite de la distancia de producto (10) se satisface para el código convolucional de producto $C^-_{[M]} \otimes C^|$ si el factor de bloqueo M satisface

$$d_B(C) = \min_{\substack{\boldsymbol{c}_1,\boldsymbol{c}_2 \in C \\ \boldsymbol{c}_1 \neq \boldsymbol{c}_2}} D_{F(D)}(\boldsymbol{c}_1,\boldsymbol{c}_2) \tag{18}$$

Ejemplo (*bloqueo*): Sea C un código convolucional (2,1) codificado con la matriz generadora básica mínima $G(D) = (1+D^2, 1+D+D^2)$. Considere el factor de bloqueo $M = 2$. La descomposición polinomial de $G(D)$ [12] es

$$G(D) = G_0 + G_1 D + G_2 D^2 = (1,1) + (0,1)D + (1,1)D^2 .$$

La correspondiente matriz generadora G semi-infinita [11] es

$$G = \begin{pmatrix} 11 & 01 & 11 & & \\ & 11 & 01 & 11 & \\ & & 11 & 01 & 11 \\ & & & \ddots & \ddots \end{pmatrix}$$

Para bloquear la matriz G, considere $M = 2$ filas de G y tome las sub-matrices 2×4 en lugar de las matrices originales 1×2, esto es

$$G_{[2]} = \begin{pmatrix} 1101 & 1100 & & \\ 0011 & 0111 & & \\ & 1101 & 1100 & \\ & 0011 & 0111 & \\ & & \ddots & \ddots \end{pmatrix}.$$

Entonces, la descomposición polinomial de $G_{[2]}(D)$ corresponde a

$$G_{[2]}(D) = \begin{pmatrix} 1,1,0,1 \\ 0,0,1,1 \end{pmatrix} + \begin{pmatrix} 1,1,0,0 \\ 0,1,1,1 \end{pmatrix} D ,$$

de lo que se tiene

$$G_{[2]}(D) = \begin{pmatrix} 1+D & 1+D & 0 & 1 \\ 0 & D & 1+D & 1+D \end{pmatrix}.$$

Generalmente, para construir un código convolucional de producto, solamente se bloquea uno de los códigos componentes.

5. DECODIFICACIÓN

Del proceso de codificación, los códigos convolucionales de producto se pueden considerar como un tipo especial de códigos convolucionales concatenados en serie. Por lo tanto, resulta adecuado aplicar un esquema de decodificación iterativo.

Los métodos de decodificación iterativos se basan en algoritmos que utilizan información sobre la confiabilidad de los símbolos de entrada y generan información sobre la confiabilidad de los símbolos de salida [13]. Estos se denominan decodificadores *soft input - soft output* (SISO). La mayoría de estos procedimientos iterativos se basan en el algoritmo de decodificación S/S-APP (*symbol by symbol a posteriori probability*) conocido como BCJR.

Para códigos concatenados el método de decodificación iterativo se adecua para reflejar la construcción del código [14]. En el caso de un esquema concatenado de dos códigos componentes, se usan dos decodificadores SISO para intercambiar información de confiabilidad correspondientes a los códigos componentes.

Como los códigos convolucionales de producto se pueden considerar como códigos convolucionales concatenados en serie con entrelazado (*interleaving*) de sus códigos componentes, se puede usar el método de decodificación iterativa para códigos concatenados en serie. Además, los códigos de producto permiten la decodificación iterativa de producto, método llamado procesamiento iterativo o filtrado MAP en [5] y [6].

La Figura 2 muestra la estructura de las palabras-código de un código convolucional de producto sistemático[1]. Esta se utiliza para ilustrar que información se pasa entre los decodificadores en los esquemas de decodificación serial y de producto que se muestran en las figuras 3 y 4, respectivamente.

Recuerde que las palabras-código de un código convolucional de producto se pueden separar en palabras-código válidas de los códigos componentes. De esta forma, independientemente del proceso de codificación, la decodificación iterativa puede realizarse decodificando los códigos componentes enen, uno primero y otro después, en forma iterativa.

[1] Un código sistemático contiene la palabra de información inalterada como parte de la palabra-código.

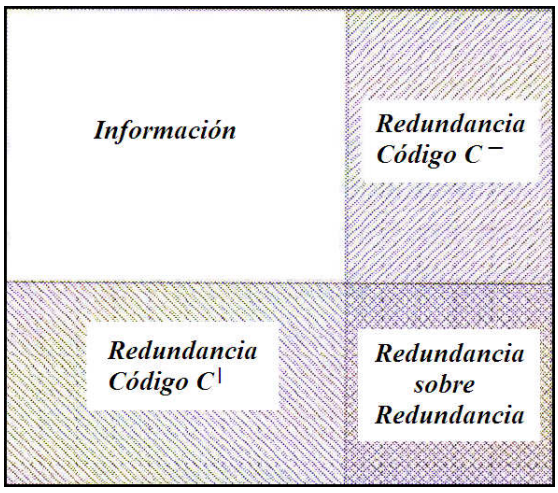

Figura 2. Estructura de palabra-código de un código convolucional de producto sistemático.

Las figuras 3 y 4 ilustran el proceso de decodificación iterativa serial y de producto, respectivamente. Note la diferencia en la información que se utiliza en el proceso de decodificación. En ambos casos se usa la palabra-código como entrada pero en cada método la información que se intercambia entre los decodificadores es diferente. En los diagramas de bloque, L_{ch} corresponde a la información de salida del demodulador después del canal, que se normaliza de acuerdo al canal. Estos valores L de canal recibidos se separan en secuencias correspondientes a los códigos constitutivos, $L_{ch}^{|}$ de $C^{|}$ y L_{ch}^{-} de C^{-}, que se usa en los decodificadores SISO del correspondiente código. L_{ext}, corresponde a los valores L extrínsecos producidos por los decodificadores y que junto con los valores L del canal, $L_{ch} + L_{ext}$ corresponden a los valores de confiabilidad de los símbolos de información de las palabras código para cada código componente. L_a son valores *a priori* para los símbolos de información que están disponibles a la salida de los decodificadores SISO y que se utilizan en el proceso iterativo.

Finalmente, después de cierto número de iteraciones hasta alcanzar la convergencia o las iteraciones que permita la aplicación (por restricciones de tiempo de procesamiento), se entregan los $L(u)$ que son los valores correspondientes a la palabra de información decodificada.

Note que en la decodificación de producto se utilizan todos los valores de la palabra-código a diferencia de la decodificación serial que sólo intercambia valores de confiabilidad de alguno de los códigos componentes.

6. EJEMPLO

Sea $C^{\otimes}$ un código convolucional de producto cuyos códigos convolucionales componentes $C^{|}$ y C^{-} son códigos (2,1) generados por la matriz codificadora básica mínima $G(D) = (1+D^2, 1+D+D^2)$ con $m = v = 2$, $d_B(C) = 2$ y $d_f = 5$.

Entonces, de la ecuación (7), se tiene que la matriz generadora $G^{\otimes}(D)$ del código de producto $C^{\otimes} = C^{-} \otimes C^{|}$, esta dada por $G^{\otimes}(D) = (1+D^4, 1+D+D^3+D^4, 1+D+D^3+D^4, 1+D^2+D^4)$. Esta es una matriz de codificación básica mínima, que tiene $m^{\otimes} = v^{\otimes} = 4$. Estos resultados están acordes con los *Teoremas* 2 y 5. Del límite en la ecuación (15) se obtiene la estimación $d_f^{\otimes} \geq 10$, cuando la distancia real del código es 13. La matriz de verificación de paridad se puede obtener de la expresión (9)

$$H^{\otimes}(D) = \begin{pmatrix} 1+D+D^2 & 1+D^2 & 0 & 0 \\ 0 & 0 & 1+D+D^2 & 1+D^2 \\ 1+D+D^2 & 0 & 1+D^2 & 0 \\ 0 & 1+D+D^2 & 0 & 1+D^2 \end{pmatrix}$$

Esta matriz es redundante, y por ejemplo, se podría eliminar la última fila de la misma.

Para incrementar la distancia libre del código de producto se puede bloquear, por ejemplo, el código vertical $C^{|}$ con un factor M. La siguiente tabla muestra la distancia libre del código de producto $C^{\otimes} = C^{-} \otimes C_{[M]}^{|}$ y la distancia estimada como función de M.

M	1	2	3	4	5	6
$d_B(C_{[M]}^{|})$	2	3	4	4	5	5
Límite (15)	10	15	20	20	**25**	25
$d_f(C^{\otimes})$	13	16	22	22	**25**	25

Tabla 1. Distancia libre del código de producto como función del factor de bloqueo M.

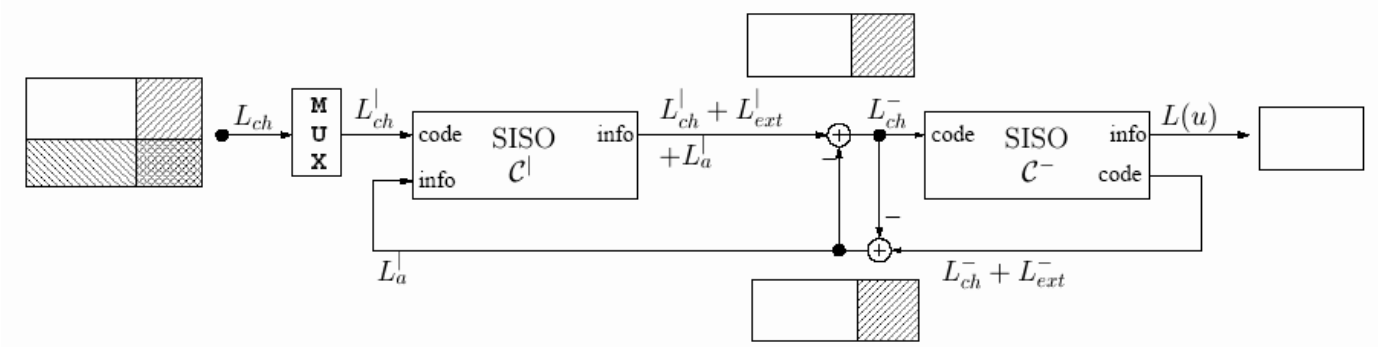

Figura 3: Diagrama de bloques de un decodificador iterativo serial para un código convolucional de producto.

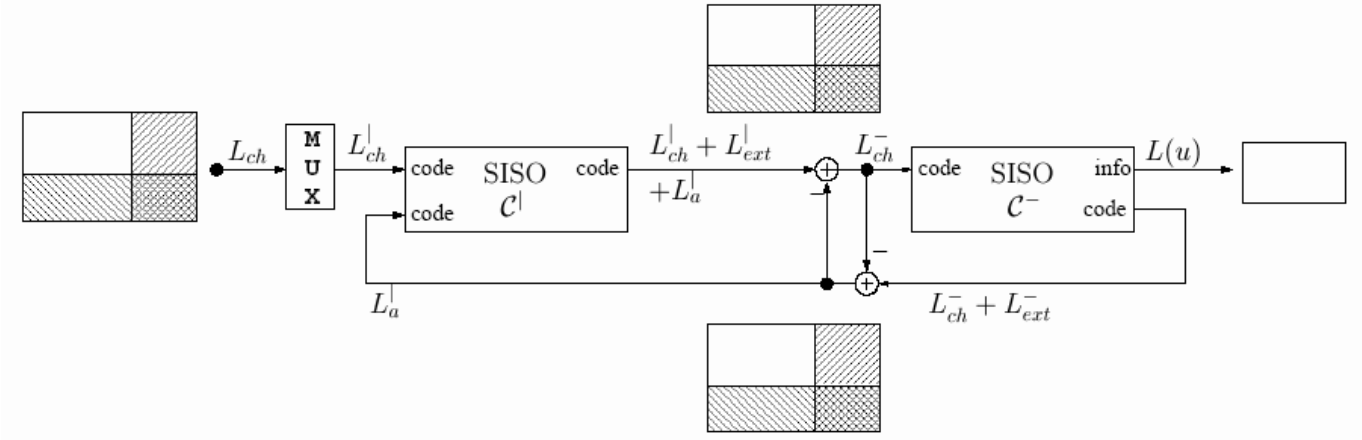

Figura 4. Diagrama de bloques de un decodificador iterativo de producto para un código convolucional de producto.

Este ejemplo muestra que la estimación de la distancia provista por la expresión (17) basada en la distancia de bloque es precisa. Como resultado, para garantizar la distancia de producto es suficiente tener un factor de bloqueo $M = 5$ dado por el *Teorema* 7. Esta mejora concuerda con el *Teorema* 10.

En la siguiente figura se compara el desempeño de la decodificación serial y de producto para el código C utilizando un factor de bloqueo $M = 10$. Aunque es suficiente un valor de $M = 5$ para alcanzar la distancia de producto, el factor M también juega el papel del tamaño del entrelazado lo cual mejora el desempeño de la decodificación iterativa. La gráfica se ha obtenido de la simulación de un sistema de comunicación que usa un código convolucional de producto con modulación BPSK a través de un canal AWGN sin memoria. Para cada razón señal a ruido, se indica la razón de error de bit (BER) después de cada iteración usando la decodificación serial y de producto. De estas curvas puede observarse que la decodificación de producto converge rápidamente (sólo se necesitan tres iteraciones) y en algunos casos tiene un mejor desempeño que la decodificación serial.

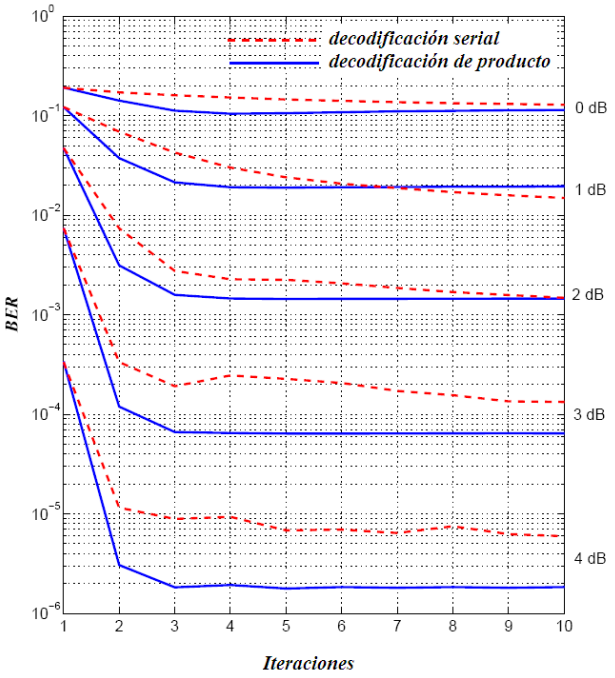

Figura 5. Comparación de los métodos iterativos de decodificación serial y de producto.

REFERENCIAS

[1] F. J. MacWilliams and N. J. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam.1992.

[2] P. Elias, "*Error Free Coding*", IRE Trans. on Inf. Theory, Vol. PGIT-4, pp 29-37, September 1954.

[3] S. Höst, *On Woven Convolutional Codes*, Ph.D. Thesis, Lund University, 1999.

[4] S. Höst and R. Johannesson and Y. Zyablov, "*Woven Convolutional Codes I: Encoder Properties*", IEEE Trans. on Inf. Theory, Vol 48, pp. 194-161, January 2002,

[5] J. Lodge, P. Hoeher, H. Hagenauet, "*The Decoding of Multidimensianal Codes using Separable MAP Filters*", Proceedings of the 6th Biennial Symposium on Communications,
Queen's University, Kingston, Ontario, Canada, pp. 343-346, May 27 -29, 7992.

[6] J. Lodge, R. Young, P. Guinand, "*Separable Concatenated Convolutional Codes: The Structure and Properties of a Class of Codes for Iterative Decoding*", European Trans. on
Telecom., Vol. 6, No.5, pp. 535-542,
Sept./Oct. 1995.

[7] M. Bossert, C. Medina, V. Sidorenko , "*Encoding and Distance Estimation of Product Convolutional Codes*", Proc. 2005 IEEE Int. Sympos. on Information Theory ISIT'05), Adelaide, Australia, pp. 1063-1067, September 4-9, 2005.

[8] G. D. Forney, Jr., "*Convolutional Codes I: Algebraic structure*", IEEE Trans. on Inf. Theory, vol. 16, pp. 720-738, November 1970.

[9] J. L. Massey, Coding Theory, Chapter 16 in Vol. 5: *Combinatorics and Geometry*, Handbook of Applicables Mathematics, Eds. W. Ledermann and S. Vajda, Publ. Wiley, Chichester, UK, 1985.

[10] Willi-Hans Steeb, *Kronecker Product of Matrices and Applications*, Manheim; Wien; Zwicb: Bl-Wissenschaftverlag.-Ver., 1991.

[11] R. Johannesson and K. Sh. Zigangirov, *Fundamentals of Convotutional Coding*, IEEE
Press, New York, 1999.

[12] R. J. McEliece, *The algebraic theory of convolutional codes*, Handbook of coding theory, Elsevier Science B.V., 1998.

[13] J. Hagenauer, E. Offer, and L. Papke, "*Iterative Decoding of Binary Block and Convolutional Codes*", IEEE Trans. on Inf. Theory, IT -42, pp.429 -445, 1996.

[14] M. Bossert, *Channel coding for Telecommunications*, John Wiley & Sons, INC. Chichester, UK, 1999.